SONICWALL TECH NOTE:

# Using the Sony PCS-1/1P with SonicWALL

## Introduction

The Sony PCS-1/1P Video Communication System provides advanced high-quality video communications and data collaboration. It used H.323 as the underlying communications protocol.

H.323 messages between terminals contain details of the IP addresses and ports that the terminals want to use for signaling and media streams. Should a terminal attempt to use private addresses to send/receive signaling or media, the connection fails because they are un-routable. By correctly configuring the SonicWALL Internet Security Appliance and Sony PCS-1/1P, these issues can be avoided.

This Tech Note details how to configure a SonicWALL Internet Security Appliance to allow use of all of the advanced features found in the Sony PCS-1/1P. The SonicWALL Internet Security Appliance may be configured to use either Many-To-One **or** One-To-One Network Address Translation (NAT) with the Sony PCS-1/1P.

This Tech Note applies **only** to the following SonicWALL Internet Security Appliances that runs Firmware version 6.x:

- GX class products
- PRO, PRO-VX, PRO 100, PRO 200, PRO 230, Pro 300, PRO 330 products
- SOHO3 and SOHO TZW class products
- TELE3 class products

This Tech Note does **not** apply to SonicWALL products that run either SonicOS 2.5.0.4 (and newer) Enhanced or Standard (such as PRO2040/3060/4060/5060 and TZ170). These products use advanced Deep Packet Transformation technology to automatically interoperate with the Sony PCS-1/1P. No configuration is needed on SonicWALL products running SonicOS 2.5.0.4 and newer for the Sony PCS-1/1P. However, NAT mode **must** be disabled on the Sony PCS-1/1P to prevent addressing conflicts when using these versions of SonicOS.

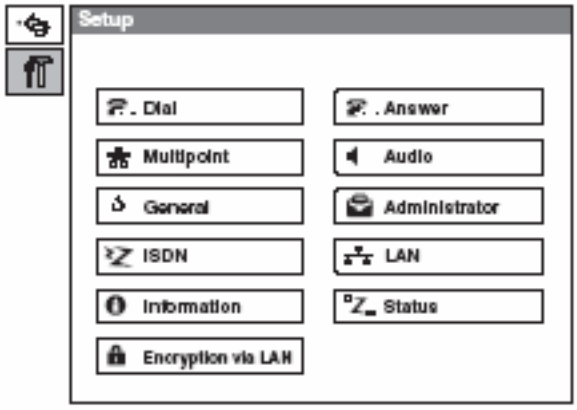
# Configuring the Sony PCS-1/1P

The Sony PCS-1/1P should be configured to operate in NAT Mode with the NAT IP Address being set to:

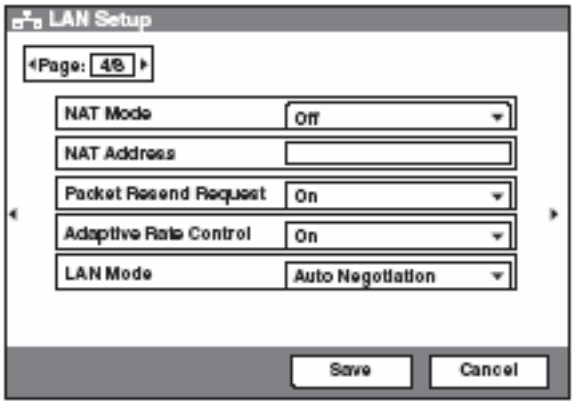
- that of the public (WAN) IP address of the SonicWALL Internet Security when it is configured to operate in Many-To-One NAT mode, or
- a dedicated public address allocated for the Sony PCS-1/P when the SonicWALL Internet Security is configured to operate in One-To-One NAT mode.

The following steps should be performed on the Sony PCS-1/1P:

1. Open the Administrator Setup Menu




2. Select the LAN Setup Menu and move to the page with NAT settings:

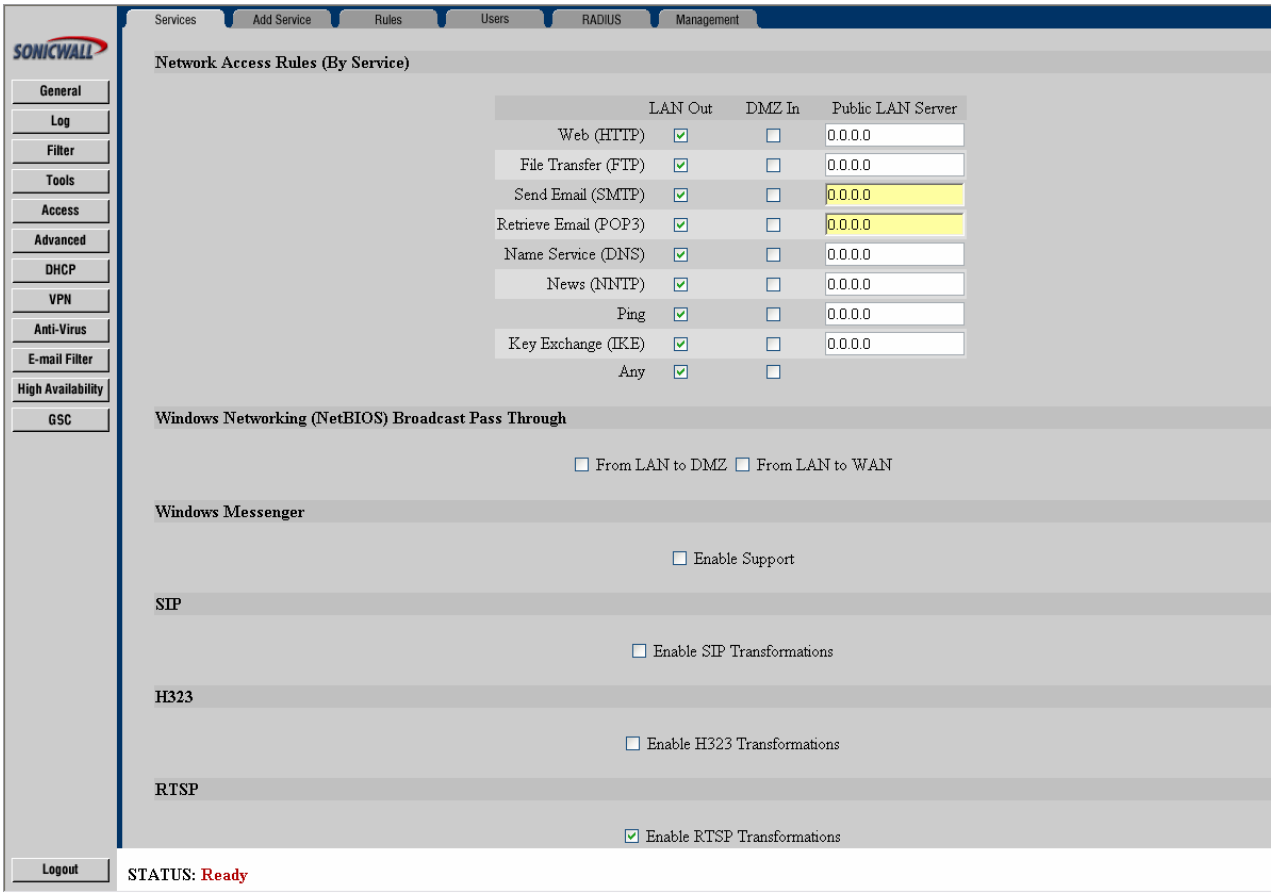



3. Use the following steps to configure NAT
   - Turn *NAT Mode* to *On.*
   - *F*ill in the *NAT Address* with the correct public IP address (see above).
   - Select *Save* when done.

# Configuring the SonicWALL

The following steps should be performed on the SonicWALL Internet Security Appliance (regardless of whether Many-To-One or One-To-One NAT is to be used):

1. Disable H.323 Transformations.
   As we will manually define the ports that the Sony PCS-1/1P will use, the integrated H.323 Transformations support within the SonicWALL need to be disabled. Use the following steps to disable H.323 transformations:
   - Click on *Access* and the *Services* tab.
   - Uncheck the *Enable H.323 Transformations* box.
   - Select the *Update* button.

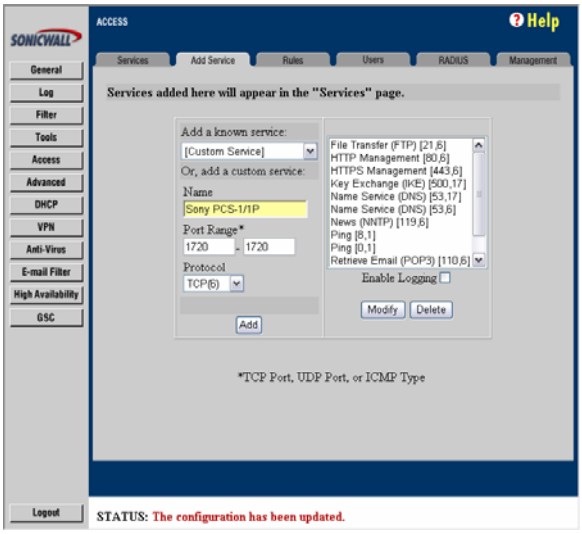



2. Add a custom service
   Create a custom service that includes all of the TCP/UDP port ranges used by the Sony PCS-1/1P. Each range of port numbers is added one by one to build up a service that covers the entire set of ranges.

   Details of the port ranges used by the Sony PCS-1/1P can be found at the end of this Tech Note.

   a. Start off by creating the custom service with the TCP port numbers used for Inbound Call Signaling. In the example shown below, we have called it 'Sony PCS-1/1P'.

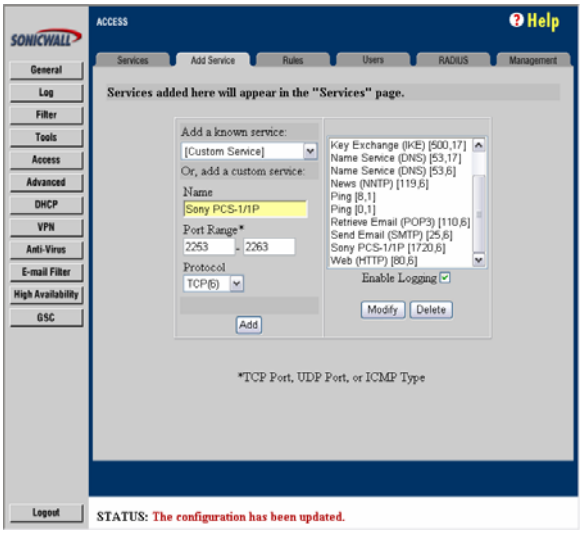
      Use the following steps to create the custom service:
      - Click on *Access* and the *Add Services* tab.
      - Fill in the *Name* field with *Sony PCS-1/1P.*
      - Fill in both the *Port Range* fields with *1720.*
      - Select *TCP* as the *Protocol.*
      - Select the *Add* button.




b. Add the TCP port range used for outbound Call Signaling to the same custom service name - 'Sony PCS-1/1P' in our example. By using the same service name, as that in the previous step, all the port ranges are tied together.

Use the following steps to extend the custom service for outbound Call Signaling:

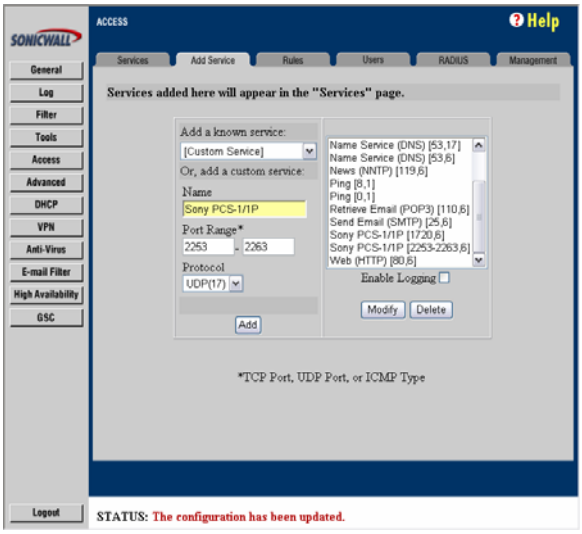
- Fill in the *Name* field with *Sony PCS-1/1P.*
- Fill in the *Port Range* fields with *2253* and *2363.*
- Select *TCP* as the *Protocol.*
- Select the *Add* button.




c. For outbound RAS, add the same port range as in the previous step, but this time specify UDP as the protocol. Again using the same service name as the previous steps. Remember to use the same service name as in the previous steps.

Use the following steps to extend the custom service for outbound RAS:

- Fill in the *Name* field with *Sony PCS-1/1P.*
- Fill in the *Port Range* fields with *2253* and *2263.*
- Select *UDP* as the *Protocol.*
- Select the *Add* button.

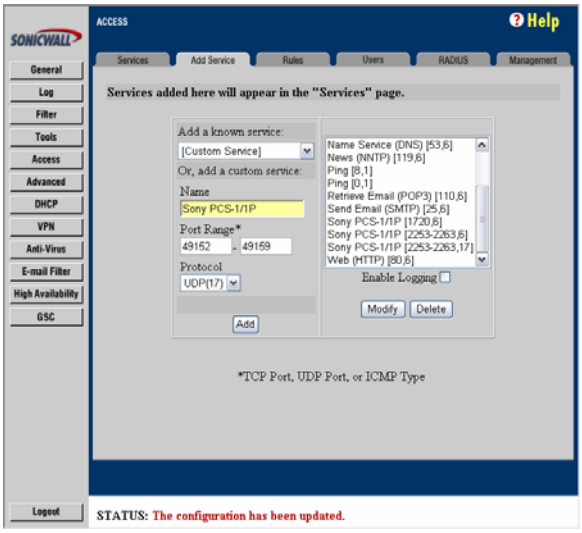



d. Finally, add the media port range to the same custom service. The actual range of port ranges added as part of this step depends on the way the Sony PCS-1/1P will be used.

When the Sony PCS-1/1P will only be used in point-to-point mode (or a caller into a multipoint conference), only a single UDP range needs to be added. . Remember to use the same service name as in the previous steps.

Use the following steps to extend the custom service for the media ports:

- Fill in the *Name* field with *Sony PCS-1/1P.*
- Fill in the *Port Range* fields with *49152* and *49159.*
- Select *UDP* as the *Protocol.*
- Select the *Add* button.




When the Sony PCS-1/1P is to be used as the main terminal for multi-point conference, a port range needs to be added for each of the possible conference participants. With the current Sony PCS-1/1P this can be up to 6 ranges, with an offset of 20 being added to the port range for each participant. This step needs to be repeated for each of the possible conference participants when using the Sony PCS-1/1P as the main terminal of a multi-point conference. Each time an offset of 20 is added to the port range, so ranges 49172-49179, 49192-49199, and so on would also be added.

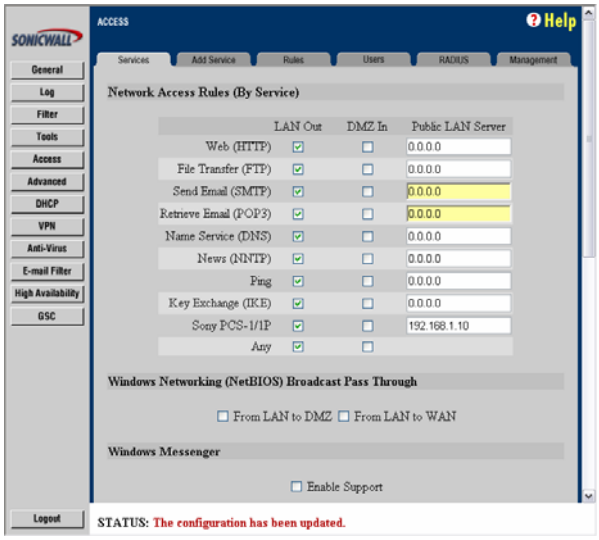
To complete the configuration of the SonicWALL Internet Security Appliance, perform **only one** of the additional stages (based on whether Many-To-One or One-To-One NAT is to be used)

- **Using Many-To-One NAT**

  Many-to-One NAT maps a subset of the TCP/UDP ports associated with the SonicWALL Internet Security Appliance (public) WAN IP address to the Sony PCS-1/1P. Using this scheme, the Sony PCS-1/1P would be accessed externally by using the SonicWALL WAN IP address – even though it is assigned a private address behind the SonicWALL Internet Security Appliance.

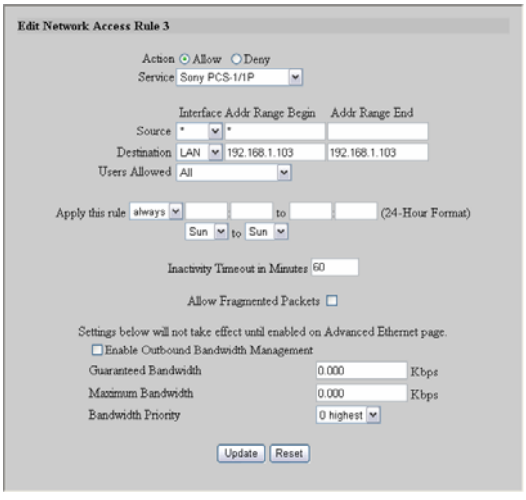
  The custom service 'Sony PCS-1/1P' created in the previous section is now enabled by associating it with the IP address of the Sony PCS-1/1P (192.168.1.10 in our example). Use the following steps to configure Many-to-One NAT:

  1. Select *Access* and then click on the *Services* tab.
  2. Fill in *192.168.1.10* in the *Public LAN Server* field associated with our custom service (*Sony PCS-1/1P*).
  3. Click *Update*.




  To ensure that calls are not terminated prematurely by the SonicWALL Internet Security Appliance, modify the timeout associated with the custom service (*Sony PCS-1/1P*) to be sufficient for your maximum call duration. Configure the following settings to define the access rule:

  1. Click *Access*, then the *Rules* tab.
  2. Click the edit icon next for the custom service we created (*Sony PCS-1/1P*)
     a. Modify the *Inactivity Timeout in Minutes* to be sufficient the maximum call duration, 60 in our example
     b. Select the *Update* button.



Setup is now complete on the SonicWALL Internet Security Appliance to use Many-To-One NAT for the Sony PCS-1/1P.

Ensure that the WAN IP address of the SonicWALL Internet Security Appliance matches that configured as the *NAT Address* on the Sony PCS-1/1P.

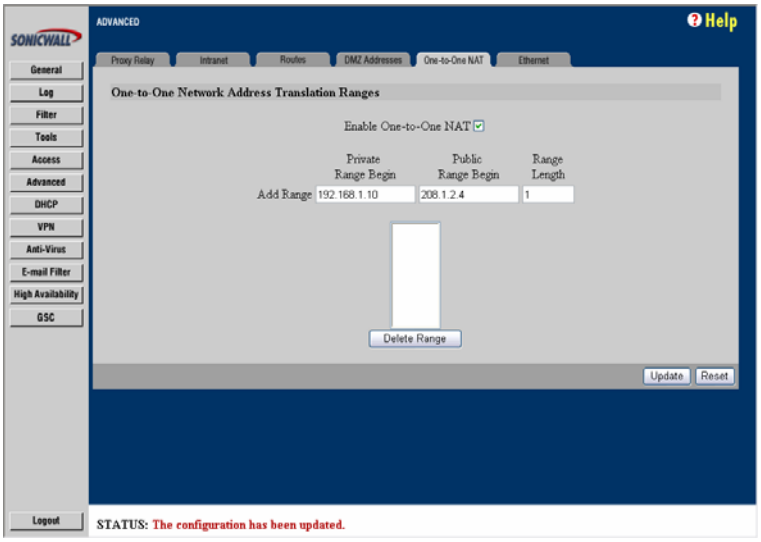
- **Using One-To-One NAT**

One-to-One NAT maps the TCP/UDP ports for a dedicated external address to a private address hidden by NAT. Using this scheme, the Sony PCS-1/1P would be accessed externally by using a dedicated public IP address – even though it is assigned a private address behind the SonicWALL Internet Security Appliance.

A One-To-One NAT mapping is setup that associates the IP address of the Sony PCS-1/1P (192.168.1.10 in our example) with a unique public IP address (208.1.2.4 in our example). The unique public IP address should not be in use by another device and match that configured as the *NAT IP Address* on the Sony PCS-1/1P.

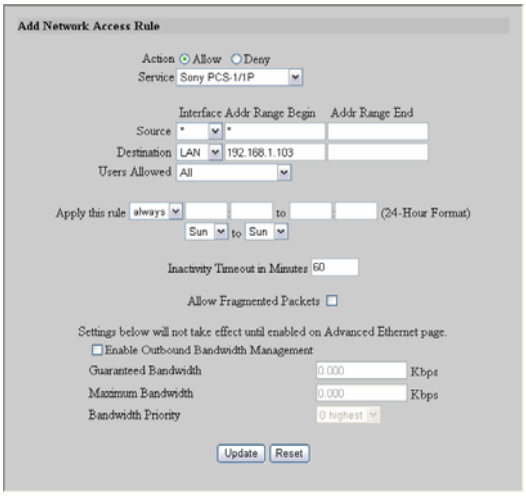
Use the following steps to configure One-to-One NAT:

1. Select *Advanced* and then click on the *One-to-One NAT* tab.
2. Select *Enable One-to-One NAT* and click *Update*.
3. Fill in *192.168.1.10* in the *Private Range Begin* field.
4. Fill in *208.1.2.4* in the *Public Range Begin* field.
5. Enter*1* in the *Range* length field.
6. Click *Update*.




Finally a rule needs to be added to allow incoming H.323 traffic for the Sony PCS-1/1P. Configure the following settings to define the access rule:

1. Click *Access*, then the *Rules* tab.
2. Click *Add New Rule* and configure the following settings:
    a) Check the *Allow* box.
    b) Specify *Service* as *Sony PCS-1/1P*, the custom service we created.
    c) Specify the *Destination* as *LAN 192.168.1.10*, the Sony PCS-1/1P in our example.
    d) Modify the *Inactivity Timeout in Minutes* to be sufficient the maximum call duration, 60 in our example
    e) Select the *Update* button.


Add Network Access Rule
Action Allow Deny
Service Sony PCS-1/1P
Interface Addr Range Begin Addr Range End
Source * *
Destination LAN 192.168.1.103
Users Allowed All
Apply this rule always to (24-Hour Format)
Sun to Sun
Inactivity Timeout in Minutes 60
Allow Fragmented Packets
Settings below will not take effect until enabled on Advanced Ethernet page.
Enable Outbound Bandwidth Management
Guaranteed Bandwidth 0.000 Kbps
Maximum Bandwidth 0.000 Kbps
Bandwidth Priority 0 highest
Update Reset

Setup is now complete on the SonicWALL Internet Security Appliance to use One-To-One NAT for the Sony PCS-1/1P.

Ensure that the unique public IP address (208.1.2.4 in our example) matches that configured as the *NAT Address* on the Sony PCS-1/1P.

## Reference

Refer to the Sony PCS-1/1P documentation for up to date information regarding port range usage.

By default, the Sony PCS-1/1P uses the following port numbers:

1. Signaling ports
   The signaling ports used are based on the firmware version being used by the Sony PCS-1/1P:

   - Version 2.4 and onwards

| Purpose | Port Range |
|---|---|
| Inbound Call Signaling (TCP) | 1720 |
| Outbound Call Signaling and RAS (TCP and UDP) | 2253-2263 |

   - Version 2.2 to Version 2.32

| Purpose | Port Range |
|---|---|
| Inbound Call Signaling (TCP) | 1720 |
| Outbound Call Signaling and RAS (TCP and UDP) | 2253-2303 |

2. Media ports (all Sony PCS-1/1P firmware versions)
   For point-to-point calls, the Sony PCS-1/1P uses the following ports:

| Purpose | Port Range |
|---|---|
| Audio | 49152-49153 |
| Video | 49154-49155 |
| Far End Camera Control | 49156-49157 |
| Data Conference | 49158-49159 |

   A Sony PCS-1/1P that is acting as the main terminal in a multi-point conference will use additional UDP media ports for each $N^{th}$ participant (after the first) of the conference:

| Purpose | Port Range |
|---|---|
| Audio | 49152 + 20 x (N – 1) |
| Video | 49154 + 20 x (N – 1) |
| Far End Camera Control | 49156 + 20 x (N – 1) |
| Data Conference | 49158 + 20 x (N – 1) |

   For example, when being using as the main terminal in a conference with three participants, the Sony PCS-1/1P will use the following port ranges: 49152-49159, 49172-49179, 49192-49199.

These port numbers can be overridden through the user interface for the Sony PCS-1/1P. The configured values being used by the Sony PCS-1/1P need to be specified on the SonicWALL Internet Security Appliance.

***Created: 8/25/2004***

***Version 1.0a***